AO 93 (Rev. 12/09) Search and Seizure Warrant (USAO CDCA Rev. 01/2013)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
One black Apple iPhone 5 cellular phone with IMEI number ~~013336004219567 and serial number F2LJGRKNF38W~~ seized on or about September 16, 2015 and currently maintained in the custody of HSI in Los Angeles, CA

Case No. 15-1768M

FILED
2015 OCT -6 PM 2:01
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES
BY

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property. Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 9/22/15 at 3:58 pm

JACQUELINE CHOOLJIAN
Judge's signature

City and state: Los Angeles, California

Hon. Jacqueline Chooljian, U.S. Magistrate Judge
Printed name and title

AUSA: L. Dotson (x4443) for A. Miller (EDVA)

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.:	*Date and time warrant executed:*	*Copy of warrant and inventory left with:*
15-1768M	September 28, 2015 (Imaged)	Searched item (: Phone 5 S/N F2LJGRKNF38W)

Inventory made in the presence of : October 6, 2015 (Searched)
Seizure Item : iPhone 5 S/N: F2LJGRKNF38W

Inventory of the property taken and name of any person(s) seized:

[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]

Items Seized / Taken:

1) One (1) Apple iPhone 5 Cellular Phone with Serial Number F2LJGRKNF38W; IMEI 013336004219567

No other Follows

Certification (by officer present during the execution of the warrant)

I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: 10/06/2015

Executing officer's signature

Robert Miyakawa Special Agent

Printed name and title

AUSA: L. Dotson (x4443) for A. Miller (EDVA)

ATTACHMENT A

PROPERTY TO BE SEARCHED

One black Apple iPhone 5 cellular phone with IMEI number 013336004219567 and serial number F2LJGRKNF38W, seized on or about September 16, 2015 and currently maintained in the custody of Homeland Security Investigations in Los Angeles, California (the "SUBJECT DEVICE").

ATTACHMENT B

ITEMS TO BE SEIZED

1. All records relating to violations of 21 U.S.C. §§ 841(a)(1) (Distribution of and Possession with Intent to Distribute a Controlled Substance) and 846 (Conspiracy to Distribute and Possess with the Intent to Distribute a Controlled Substance), those violations involving JOSE ALFONSO ROMERO-RAMIREZ, and other co-conspirators known and unknown, specifically:

a. Address book and other contact information, including stored and saved telephone numbers, addresses, and email addresses;

b. Call log information, including all phone numbers dialed from the SUBJECT DEVICE as well as all received or missed incoming calls between August 1, 2014 and September 16, 2015;

c. Short Message Service ("SMS") texts and other text communications sent or received from the SUBJECT DEVICE relating to narcotics trafficking into the United States between August 1, 2014 and September 16, 2015;

d. Email or other communications sent or received from the SUBJECT DEVICE relating to narcotics trafficking into the United States between August 1, 2014 and September 16, 2015;

e. Photographs or videos of individuals, documents and other records, places, and things relating to narcotics trafficking into the United States; and

f. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes,

destinations, origination points, and other locations, between August 1, 2014 and September 16, 2015.

2. The SUBJECT DEVICE, which was used to facilitate the above-listed violations (and forensic copies thereof).

3. With respect to any SUBJECT DEVICE used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

SEARCH PROCEDURE FOR DIGITAL DEVICE

4. In searching the SUBJECT DEVICE (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search the SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE as soon as is practicable but not to exceed 60 days from the date of issuance of the warrant. If additional

time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

e. The search team shall make and retain notes regarding its search of the SUBJECT DEVICE.

f. If the search team, while searching a SUBJECT DEVICE, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that SUBJECT DEVICE pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence

of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

g. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

h. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

i. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the SUBJECT DEVICE but may not access them (after the time for searching the device has expired) absent further court order.

j. The government may retain a SUBJECT DEVICE itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the SUBJECT DEVICE is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the SUBJECT DEVICE (or while an application for such an order is pending). Otherwise, the government must return the SUBJECT DEVICE.

k. Notwithstanding the above, after the completion of the search of the SUBJECT DEVICE, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

2. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Robert Miyakawa, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"). I am currently assigned to the Los Angeles Gang Investigation Group and have been employed by ICE, or its predecessor entity, since 2009. Among other duties, HSI is responsible for enforcing federal criminal statutes prohibiting the possession and distribution of controlled substances.

2. During the course of my employment with ICE, I have received classroom and on-the-job training in federal criminal law, customs law, and immigration and nationality laws of the United States. As an SA, I have conducted and participated in numerous investigations involving narcotics distribution and sales, as well as human smuggling, counterfeit documents, employer sanctions, benefits fraud, and re-entry after deportation. Through these investigations, I have questioned suspects and witnesses, reviewed evidence, conducted surveillance, and executed arrest and search warrants.

II. PURPOSE OF AFFIDAVIT

3. On April 21, 2015, in a superseding indictment in case no. 3:15CR043-JRS in the Eastern District of Virginia, JOSE ALFONSO ROMERO-RAMIREZ, also known as ("aka") "El Tio," aka "Oscar Romero," ("ROMERO-RAMIREZ") was charged with Conspiracy

to Distribute and Possess with Intent to Distribute 50 Grams or More of Methamphetamine, in violation of 21 U.S.C. § 846. An arrest warrant was issued for ROMERO-RAMIREZ on March 18, 2015 when the indictment was originally filed.

4. This affidavit is made in support of an application for a warrant to search the digital device (the "SUBJECT DEVICE"), as described in Attachment A, that was seized from ROMERO-RAMIREZ at the time of his arrest on or about September 16, 2015 in the Central District of California, and which is currently in the custody of HSI. The list of items to be seized is set forth in Attachment B. Attachments A and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of, or investigation into, this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. PROPERTY TO BE SEARCHED

6. The property to be searched, as described in Attachment A which is incorporated herein by reference, is one black Apple iPhone 5 cellular phone with IMEI number 013336004219567 and serial number F2LJGRKNF38W, seized on or about September 16, 2015 and currently maintained in the custody

of Homeland Security Investigations in Los Angeles, California (the "SUBJECT DEVICE").

IV. ITEMS TO BE SEIZED

7. The requested search warrant seeks authorization to seize any data on the SUBJECT DEVICE that constitutes evidence or fruits of violations of 21 U.S.C. §§ 841(a)(1) (Distribution of and Possession with Intent to Distribute a Controlled Substance) and 846 (Conspiracy to Distribute and Possess with the Intent to Distribute a Controlled Substance) (collectively, the "SUBJECT OFFENSES"), and the SUBJECT DEVICE, which is itself an instrumentality of the SUBJECT OFFENSES.

V. SUMMARY OF PROBABLE CAUSE

8. Based on my conversations with HSI SA Matthew Rosenberg ("SA Rosenberg"), the agent handling the investigation of ROMERO-RAMIREZ and his co-defendants in the Eastern District of Virginia, I am aware that ROMERO-RAMIREZ is one of several drug dealers who distributed methamphetamine supplied by co-defendant LUIS MENDEZ ("MENDEZ"). On September 16, 2015, I arrested ROMERO-RAMIREZ pursuant to the arrest warrant issued in the Eastern District of Virginia. Upon conducting a search incident to arrest, I found the SUBJECT DEVICE on ROMERO-RAMIREZ's person. Based on my training and experience and debriefings with other law enforcement officers and agents, I am aware that ROMERO-RAMIREZ is a drug trafficker who has used a cellular phone in the past to facilitate drug transactions and believe that there is probable cause to conclude that the SUBJECT DEVICE contains evidence or fruits of violations of the

SUBJECT OFFENSES and is itself an instrumentality of the SUBJECT OFFENSES.

VI. STATEMENT OF PROBABLE CAUSE

A. Background

9. Based on my conversations with SA Rosenberg and other agents, I am aware of the following:

a. Beginning in February 2014, a confidential informant (the "CI")[1] began communicating with MENDEZ regarding the purchase of methamphetamine in Richmond, Virginia.[2]

b. In controlled, monitored purchases in February, March, and April of 2014, MENDEZ sold the CI a total of 93.6 grams of a mixture and substance containing methamphetamine with a purity of over 90%.

c. On May 24, 2014, MENDEZ told the CI that he had moved back to Los Angeles, California but was willing to sell the CI more methamphetamine through the mail. The CI then introduced MENDEZ to an undercover agent (the "UC"), who later purchased additional methamphetamine and a weapon through one of MENDEZ's intermediaries in Richmond, Virginia.

---

[1] According to SA Rosenberg, the CI has received compensation for his/her involvement in this investigation and has been provided immigration benefits, including the opportunity to remain in the United States during this investigation. SA Rosenberg stated that the CI has no criminal convictions and, to his knowledge, has not been involved in any unauthorized criminal activity while engaged as an informant.

[2] According to SA Rosenberg, all conversations referenced in this affidavit involving MENDEZ or ROMERO-RAMIREZ were primarily in Spanish. SA Rosenberg does not speak fluent Spanish and has relied on translations and transcripts, as well as debriefings with other agents and the CI who speak Spanish, to understand the content of these communications.

d. On September 24, 2014, the UC texted MENDEZ regarding the purchase of additional methamphetamine. MENDEZ told the UC that a man named "El Tio" (later identified as ROMERO-RAMIREZ)[3] could supply methamphetamine at a restaurant called "El Tio Tienda Y Restaurante" (the "restaurant") located at 4800 Jefferson Davis Highway in Richmond, Virginia.

B. ROMERO-RAMIREZ Sells Two Ounces of Methamphetamine to an Undercover Agent on October 27, 2014

10. Based on my conversations with SA Rosenberg, I am aware of the following:

a. Between October 13, 2014 and October 26, 2014, MENDEZ and the UC again exchanged text messages regarding the purchase of methamphetamine. MENDEZ and the UC agreed to conduct a methamphetamine transaction on October 27, 2014. They agreed that ROMERO-RAMIREZ and the UC would conduct the transaction at the restaurant.

b. Toll records from MENDEZ's phone show that between October 15, 2014 and October 27, 2014, there were multiple phone calls and text messages between MENDEZ's phone and a phone registered through AT&T to ROMERO-RAMIREZ and believed to be used by ROMERO-RAMIREZ. On October 27, 2014, the day of the methamphetamine transaction, toll records show that MENDEZ and ROMERO-RAMIREZ were in contact approximately eight

[3] Based on statements by Federal Bureau of Investigation ("FBI") SA Catherine Nowery, I am aware that the UC reviewed the booking photograph of ROMERO-RAMIREZ following his arrest on September 16, 2015. The UC confirmed that ROMERO-RAMIREZ is the man known throughout the investigation as "El Tio" and from whom the UC purchased methamphetamine.

times.

c. On or about October 27, 2014, during a monitored, controlled purchase, the UC met ROMERO-RAMIREZ in the parking lot of the restaurant to conduct the methamphetamine transaction. Upon arrival, the UC and ROMERO-RAMIREZ walked to the rear of the parking lot, where ROMERO-RAMIREZ opened the door of a parked van with no license plates. ROMERO-RAMIREZ briefly got inside of the van and pointed to a white cup containing approximately two ounces of methamphetamine. Upon exiting the van, ROMERO-RAMIREZ handed the white cup with the methamphetamine to the UC. The UC then got inside of the van, counted the money, and at the direction of ROMERO-RAMIREZ, left $3,000 in the cup holder of the van. The UC exited the van, shook hands with ROMERO-RAMIREZ, and left the area with the white cup containing the methamphetamine.

d. The United States Customs and Border Protection laboratory report confirmed the presence of methamphetamine in the mixture and substance ROMERO-RAMIREZ sold to the UC. The net weight was 54.5 grams, or approximately two ounces. The purity was over 90%.

C. Agents Arrest ROMERO-RAMIREZ and Seize the SUBJECT DEVICE on September 16, 2015 in the Central District of California

11. As stated, ROMERO-RAMIREZ was charged in the Eastern District of Virginia with Conspiracy to Distribute and Possess with Intent to Distribute 50 Grams or More of Methamphetamine, in violation of 21 U.S.C. § 846. An arrest warrant was issued in that district.

12. On September 16, 2015, I arrested ROMERO-RAMIREZ in the Central District of California. I conducted a search incident to arrest and located the SUBJECT DEVICE. The SUBJECT DEVICE has not yet been searched.

13. Based on my training and experience, drug traffickers frequently communicate with drug couriers and distributers via cellular devices, including text messages and email messages. Indeed, in this case, toll records show that MENDEZ and ROMERO-RAMIREZ communicated through phone calls and text messages. Furthermore, based on my training and experience, I know that individuals are likely to retain videos, photographs, emails, text messages, and other forms of digital communications and evidence on their cellular telephones. For these reasons, I believe there is probable cause to conclude that evidence regarding the drug trafficking activities of ROMERO-RAMIREZ, MENDEZ, and possibly other co-conspirators involved in MENDEZ's drug distribution network is likely to be found on the SUBJECT DEVICE.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

14. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives

intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it takes time to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, operating system, and software application being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory

or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes ("GB") of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 240 million pages of data, that, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 GB drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack

space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in

digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be

necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

///

///

///

VIII. CONCLUSION

15. For the reasons described above, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, as described in Attachment B, will be found on the SUBJECT DEVICE.

ROBERT MIYAKAWA,
Special Agent, Homeland
Security Investigations

Subscribed to and sworn before me
this ____ day of September, 2015.

HONORABLE JACQUELINE CHOOLJIAN
UNITED STATES MAGISTRATE JUDGE